Entanglement-free certification of entangling gates

Marcelo de Almeida[1,2], Mile Gu[3,4], Alessandro Fedrizzi[1,2], Matthew A. Broome[1,2],
Timothy C. Ralph[2], and Andrew G. White[1,2]

[1]*Centre for Engineered Quantum Systems,* [2]*Centre for Quantum Computer and Communication Technology,*
School of Mathematics and Physics, University of Queensland, Brisbane, QLD 4072, Australia
[3]*Centre for Quantum Technologies, National University of Singapore, Singapore*
[4]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China.*

Not all quantum protocols require entanglement to outperform their classical alternatives. The nonclassical correlations that lead to this quantum advantage are conjectured to be captured by quantum discord. Here we demonstrate that discord can be explicitly used as a resource: certifying untrusted entangling gates without generating entanglement at any stage. We implement our protocol in the single-photon regime, and show its success in the presence of high levels of noise and imperfect gate operations. Our technique offers a practical method for benchmarking entangling gates in physical architectures in which only highly-mixed states are available.

Models of intermediate quantum computing [1–4] offer an intriguing approach for developing quantum devices that outperform their classical counterparts. These models derive their attraction from the reduced resources compared to scalable quantum computing, and hence should be realisable sooner. One example of intermediate quantum computation is the mixed-state algorithm DQC1 [1]. Its computational advtange is often [5, 6] associated with *quantum discord* [7, 8], a nonclassical correlation which is identical to entanglement for pure states, but persists for mixed states, even when the entanglement is zero.

The presence of such nonclassical correlations in virtually all mixed states prompted the question as to whether discord was ultimately a useful quantum resource [9]. While it is now known that quantum circuits consisting of one- and two-qubit gates cannot provide superpolynomial computational speedups without generating discord [10], a formal link to computational advantage of specific protocols such as DQC1 is still missing. This has motivated much effort in identifying the operational significance of discord, both in theory [11–20] and experiment [21, 22]. Most recently, it has been shown that discord can be consumed as a resource to encode information that only coherent interactions can extract [22].

Here we show that discord has a direct practical application. We use it to verify that an untrusted party can implement two-qubit entangling operations. This is often hard to achieve: since the generation of pure probe states—separable or entangled—is difficult in many physical architectures, thus our technique significantly lowers the bar for verifying entangling operations. We test our technique using a two-qubit photonic entangling gate and show that we can verify entangling operation even in the presence of environmental noise or imperfect gates.

In the *discord consumption* protocol introduced in [22], Alice randomly encodes information in some discordant bipartite state ρ_{AB}, and Bob is challenged to retrieve as much of this information as possible. If Bob is limited to performing a single local measurement on each bipartition, then his performance is constrained to some incoherent limit. However, Bob can surpass this classical limit by harnessing discord present in the system through coherent bipartite interactions. The protocol suggested that discord could be used to test for Bob's capacity to coherently interact, and thus entangle the two physical systems. The continuous-variable implementation of [22], however, contained a loophole. The incoherent limit assumed that each bipartition was measured only once. Bob could thus potentially cheat and surpass this bound through multiple rounds of measurements with a degenerate spectrum.

The loophole can be closed if Alice's bipartite state consists of two discordant *qubits*. Here we show that the incoherent limit strictly bounds the amount of information Bob can access with only single-qubit quantum gates. Should Bob surpass this limit, Alice can be certain that Bob has an entangling two-qubit gate.

Alice first prepares a two-qubit state ρ_{AB} in an equal mixture of the three symmetric Bell states,

$$\rho_{AB} = \frac{1}{3}\left(|\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-| + |\psi^+\rangle\langle\psi^+|\right), \qquad (1)$$

where $|\phi^\pm\rangle{=}(|00\rangle{\pm}|11\rangle)/\sqrt{2}$ and $|\psi^\pm\rangle{=}(|01\rangle{\pm}|10\rangle)/\sqrt{2}$. This state can be rewritten as $\rho_{AB}{=}\sum_i(|0_i0_i\rangle\langle 0_i0_i| + |1_i1_i\rangle\langle 1_i1_i|)$, where $i{=}\{x,y,z\}$, so that $|0\rangle_i$ and $|1\rangle_i$ represent the computational basis states with respect to the Pauli operators σ_i. Thus, ρ_{AB} can always be prepared by initialising two qubits oriented in one of the six orthogonal directions on the Bloch sphere at random. The state ρ_{AB} is thus clearly separable, but contains non-zero discord.

Discord aims to capture solely the quantum component of the correlations between two physical systems [7, 8]. The total correlations between two systems, A and B, are quantified by the mutual information $I(A,B){=}S(\rho_A){+}S(\rho_B){-}S(\rho_{AB})$. Meanwhile the classical component of these correlations, $J(A|B){=}S(\rho_A){-}\max_{\{\Pi_b\}\in\mathcal{M}}\sum p_b S(\rho_{A|b})$, is defined by the reduction in the entropy of A after a measurement on B, when maximized over positive operator value measurements (POVMs) performed on B. (Here, p_b is the probability of getting measurement outcome b, leaving A in the conditional state $\rho_{A|b}$, and $\mathcal{M}$ represents the class of all possible POVMs). Thus, the difference between these quantities quantifies the amount of quantum correlations between A and B. We define this discrepancy, $\delta(A|B){=}I(A,B){-}J(A|B)$, as the discord. For our protocol, we find $\delta(A|B){=}\delta(B|A){=}\frac{1}{3}$.

To test Bob's capacity to implement entangling gates, Alice first generates a random variable $\mathbf{K}$ that is uniformly distributed between the four possible values (b_1, b_2), where $b_1, b_2 \in \{0, 1\}$ are random bits, Fig. 1a). She encodes each possible $k = (b_1, b_2)$ on her system by application of the corresponding local unitary $U_k = \sigma_x^{b_1}\sigma_z^{b_2}$ on qubit A. The qubit pair is given to Bob, who is challenged to guess k by returning an estimate k_m governed by a random variable $\mathbf{K}_m$. Bob's performance is then quantified by the amount of information k_m contains about k, i.e., $I_{\text{exp}} = I(\mathbf{K}, \mathbf{K}_m)$, where $I(\mathbf{K}, \mathbf{K}_m)$ is the mutual information between $\mathbf{K}$ and $\mathbf{K}_m$.

Let I_c be Bob's best possible performance when he is restricted to single-qubit gates and single qubit measurements. Let I_q be his performance when he can also implement arbitrary two-qubit gates on A and B, or between either qubit and additional ancilla qubits: $\Delta I{=}I_q{-}I_c$ is then the 'quantum advantage' of having two-qubit entangling gates. Provided ΔI is non-zero, Alice can be certain that Bob possesses some entangling two-qubit gate. In the appendix, we show that this is possible for *any general* two-qubit state ρ_{AB} that contains discord. Furthermore, provided A and B represent qubits,

$$I_q - I_c = \delta(A|B). \tag{2}$$

The amount of information Alice can encode within ρ_{AB} that can be accessed by two-qubit operations is given exactly by the amount of discord in ρ_{AB}.

Bob's optimal strategy is to perform a Bell state measurement on the state he receives from Alice. For each k, the resulting state after application of U_k will be an equal mixture of three of the four Bell states

$$\rho_{AB} = \frac{1}{6}\begin{bmatrix} 2{-}b_1 & 0 & 0 & b_1 r \\ 0 & 1{+}b_1 & (1{-}b_1)r & 0 \\ 0 & (1{-}b_1)r & 1{+}b_1 & 0 \\ b_1 r & 0 & 0 & 2{-}b_1 \end{bmatrix} \tag{3}$$

where $r{=}(-1)^{b_2}$. For every instance of the protocol, Bob's Bell state measurement will thus allow him to eliminate one of the four possible values of k. His probability of correctly guessing k based on each outcome will be $1/3$, which results in an information rate of $I_q{=}2{-}\log_2(3) \approx 0.415$, assuming zero noise and a perfect gate operation.

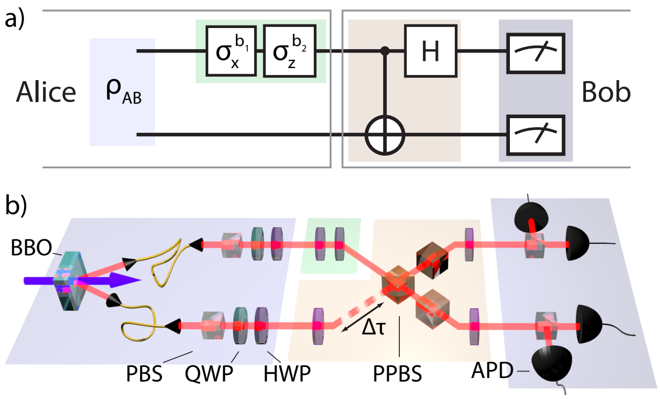

FIG. 1. a) Quantum circuit representation of the protocol. Alice prepares discordant state ρ_{AB} and encodes onto it the classical quaternary variable k via the unitaries $\sigma_x^{b_1}$, $\sigma_z^{b_2}$. Bob conducts an allegedly entangling operation—optimally a Bell-state measurement—to estimate Alice's encoding. b) Experiment. Alice's qubits are realised using orthogonal polarisation states of two 820 nm single photons generated via type-I spontaneous parametric down-conversion in a 2 mm β-barium-borate (BBO) crystal pumped by a frequency-doubled Ti:Sapphire laser (820 nm → 410 nm, 100 fs at 76 MHz). Her single-qubits are initialised with polarising beamsplitters (PBS), and rotated (lilac area) and encoded (green area) via quarter- (QWP) and half-wave plates (HWP). Bob's entangling measurement is realised with a non-deterministic CZ gate based on nonclassical interference of photons at a partially-polarising beam splitter (PPBS) of reflectivity $\eta_V = 2/3$ ($\eta_H = 0$) for vertical (horizontal) polarisation. Photon arrival time is controlled by a relative temporal delay $\Delta\tau{=}0$, which is used to tune gate quality. The three HWPs enact Hadamard operations to turn the CZ into a CNOT gate, and to complete the Bell-state measurement (yellow area). Photons are analysed in detected in the Z-basis by PBS's, and detected by avalanche photodiodes (APD, grey area).

In contrast, Bob's maximal information rate *without* an entangling two-qubit gate is bounded above by $I_c = I_q{-}\delta(A|B){=}5/3{-}\log_2(3){\approx}0.082$ for our particular ρ_{AB}. Upon receipt of k_m, Alice can compute Bob's achieved information rate I_q^{exp}. Should this exceed I_c, she is sure that Bob is capable of implementing an entangling two-qubit operation.

In our experiment, Alice encodes ρ_{AB} in the polarisation of two single photon qubits, where horizontal $|H\rangle$ and vertical $|V\rangle$ polarisations correspond to the logical states $|0\rangle$ and $|1\rangle$, Fig. 1b). Bob conducts his Bell-state measurements using a non-deterministic, controlled-phase (CZ) gate [23, 24] and single-qubit Hadamard gates. The CZ gate relies on two-photon interference at a beamsplitter, imparting a π phase shift on the input state $U_{\text{CZ}}|VV\rangle \rightarrow -|VV\rangle$, while leaving other input combinations of these basis states unchanged.

Alice constructs her discordant state ρ_{AB} sequentially by preparing photons in one of the states $\{|HH\rangle, |VV\rangle, |DD\rangle, |AA\rangle, |RR\rangle, |LL\rangle\}$, where $|D\rangle, |A\rangle=(|H\rangle\pm|V\rangle)/\sqrt{2}$ and $|R\rangle, |L\rangle=(|H\rangle\pm i|V\rangle)/\sqrt{2}$, and applies one of the four encodings k. Bob's Bell state measurement sums up over all components of Alice's state to extract the final measurement outcomes. The experimental information rate achieved was $I_q^{\rm exp}$=0.363±0.008 which is more than 35 standard deviations above the classical limit for I_c.

We investigated the robustness of the protocol by studying two key sources of imperfection: i) the addition of white noise to the ideal state, $\tilde{\rho}_{AB}$=$p\ \rho_{AB}$+$(1-p)\ \frac{\mathbb{1}}{4}$; and ii) imperfect gate operation, by increasing the temporal distinguishability between the two interfering photons, $\Delta\tau$. We modelled the latter by mixing one of the input photon modes of the gate with a vacuum mode using a virtual beamsplitter with variable transmission ξ [23]: the relation of this parameter to the temporal mismatch $\Delta\tau$ is found by mapping to the well-known Gaussian two-photon interference pattern, ξ=$1-e^{-(\Delta\omega\Delta\tau)^2}$, where $\Delta\omega$ is the spectral bandwidth of our single photons. Starting from Bob's optimal information rate I_q≃0.415, Fig. 2(a) predicts a large operating range with quantum advantage.

We tested this prediction experimentally. In Fig. 2(b) Bob runs the entangling gate optimally, $\Delta\tau$=0, and Alice increases the noise on her state until $\tilde{\rho}_{AB}$ is fully mixed. As predicted, we find that Bob *always* retains a quantum advantage over the classical estimate for a given level of noise.

In Fig. 2(c) Alice prepares the optimal state ρ_{AB} and Bob decreases gate performance by temporal mode mismatch. The amount of information that can be extracted without two-qubit gates, I_c, in this scenario is independent of the gate operation and thus constant. Again, as predicted, Bob can demonstrate a quantum advantage up to ~ 0.1 coherence lengths: Bob can still convince Alice he is capable of performing an entangling operation even when his gate doesn't perform very well. Conversely, if Alice knows the quality of the states she sent, she will be able to quantify the performance of Bob's entangling gate based on his guess.

Our technique could be particularly useful for characterising physical architectures that are intrinsically entangling—such as spins in a solid interacting via J-coupling—but where initialising the qubits to a pure state is difficult. Our experiment demonstrates that in such architectures mixed-states containing discord above the classical bound I_c suffice to certify entangling operation.

We thank G. G. Gillett for help with data acquisition, K. Modi and V. Vedral for helpful discussions. This work was supported in part by the Centre for Engineered Quantum Systems (CE110001013) and the Centre for Quantum Computation and Communication Technology (CE110001027). AGW and TCR were supported by Uni-

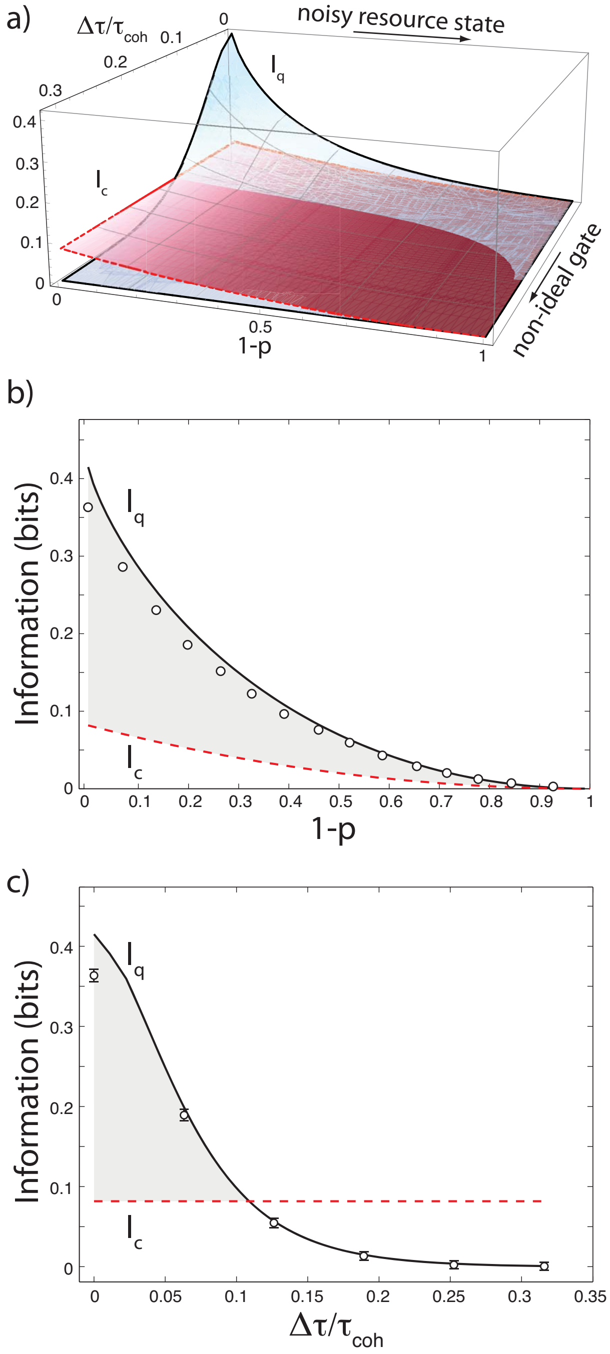

FIG. 2. Certification of a quantum operation with discordant states. (a) Theoretical performance I_q achievable by Bob with arbitrary two-qubit gates as a function of noise in Alice's resource states, $1-p$, and of the quality of Bob's gate operation, $\Delta\tau/\tau_{coh}$. (b) Experimental results. Using a (CZ) gate, Bob will always do better than someone with only single-qubit gates when Alice sends noisy discordant input states $\tilde{\rho}_{AB} = p\rho_{AB} + (1-p)\frac{\mathbb{1}}{4}$. The shaded regions represent the theoretical quantum advantage. Error bars are smaller than symbol size. (c) Bob retains this advantage when using a less-than-ideal (CZ) gate, experimentally realized via temporal mode mismatch $\Delta\tau/\tau_{coh}$ between the interacting photonic qubits, up to $\Delta\tau/\tau_{\rm coh} = 0.1$. Errors are based on Poissonian counting statistics.

versity of Queensland Vice-Chancellor's Senior Research Fellowships. MG was supported by the Ministry of Education in Singapore.

Appendix A: Proof of main result

In this section, we prove that for an arbitrary two-qubit state ρ_{AB} with discord $\delta(A|B)$, and the aforementioned encoding, Bob's advantage using entangling gates is

$$I_q - I_c = \delta(A|B), \tag{4}$$

where I_q is Bob's optimal performance with arbitrary quantum processing, and I_c is is optimal performance when entangling two-qubit gates are unavailable. To do this, we introduce an additional scenario. Let I_c' be Bob's optimal performance when he has no entangling gates, and furthermore, is restricted to a single measurement on each qubit. Clearly this addition restriction implies that $I_c' \leq I_c$. We will prove that additionally, $I_c \leq I_c'$, and thus $I_c = I_c'$.

This is done by contradiction. Assume that $I_c > I_c'$, i.e., Bob can exceed a performance of I_c' without use of entangling gates by making multiple measurements on either qubit A or qubit B. Let this be qubit A without loss of generality.

Since A resides in a 2-dimensional Hilbert space, subsequent measurements on A are advantageous only if the first was weak, i.e., involving the interaction of A with an ancilla C, followed by a measurement of C. This interaction, however, must have the potential to entangle A and C and thus constitutes an entangling gate. This contradicts out assumption that Bob did not use entangling gates. Therefore $I_c = I_c'$.

In [22], I_c' is referred to as the *incoherent limit*, and it was established that

$$I_q - I_c' = \Delta(A|B) \tag{5}$$

provided Alice's choice of encoding is maximal ($\sum_k p_k U_k \rho U^k = \mathbf{I}/2$ is totally mixed for any single qubit state ρ). This condition is satisfied for the encoding in our protocol, thus, the relation also applies to I_c. Thus $I_q - I_c = \delta(A|B)$.

Appendix B: Explicit Evaluation of I_c

Here we explicitly show that for the specific protocol where ρ_{AB} is a mixture of three Bell states, Bob's optimal performance without two-qubit gates is $I_c = \frac{5}{3} - \log_2(3)$. First, note that Bob can saturate I_c by making a single σ_z measurement on each of two qubits he receives from Alice. If the measurement results are identical, he guesses $k = (0, ?)$, otherwise he guesses $k = (1, ?)$, where ? denotes a random guess. This strategy gives no information about the second bit, but can guess the first bit correctly 2/3 of the time. The resulting information rate is $1 - H(\frac{1}{3}) = I_c$, where $H(.)$ denotes the binary entropy.

This strategy is in fact optimal. We note from Appendix A that Bob's optimal strategy need only involve a single measurement on each qubit. Consider first a measurement on system B described by operators $\{\Pi_b\}$. Since the encoding U_k is localized to A, it commutes with the measurement operation. Therefore, if Bob were to get measurement outcome b, Alice would have effectively encoded onto the conditional state $\rho_{A|b}$. Bob's resulting information rate is thus constrained by the Holevo bound, $1 - \sum_b p_b S(\rho_{A|b})$, which is maximized when Bob chooses a measurement that minimizes the expected entropy of the resulting state. Due to the symmetry of ρ_{AB}, any projective measurement does this. Without loss of generality, measurement in the Z basis gives

$$S(\rho_{A|b}) = \sigma_x^b \left(\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1| \right) \sigma_x^b \tag{6}$$

This results in a Holevo bound of $1 - H(\frac{1}{3}) = \frac{5}{3} - \log_2(3)$.

To bound the case where Bob decides to measure qubit A, we note that Bell states satisfy the property $(\sigma_x^{b_1}\sigma_z^{b_2} \otimes I)\rho_{AB}(\sigma_x^{b_1}\sigma_z^{b_2} \otimes I) = (I \otimes \sigma_x^{b_1}\sigma_z^{b_2})\rho_{AB}(I \otimes \sigma_x^{b_1}\sigma_z^{b_2})$. That is, although Alice encoded onto qubit A, the resulting state is functionally equivalent to encoding on qubit B. Thus, by inverting A and B, the previous argument applies.

The optimal performance Bob can achieve without entangling two-qubit gates is therefore $I_c = \frac{5}{3} - \log_2(3)$. Since $\delta(A|B) = 1/3$, this agrees with our general result that $I_q - I_c = \delta(A|B)$.

[1] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).

[2] S. Jordan, Quantum Information & Computation **10**, 470 (2010).

[3] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science **467**, 459 (2011).

[4] S. Aaronson and A. Arkhipov, Proc. ACM Symposium on Theory of Computing, San Jose, CA , 333 (2011).

[5] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).

[6] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White, Phys. Rev. Lett. **101**, 200501 (2008).

[7] L. Henderson and V. Vedral, Journal of Physics A: Mathematical and General **34**, 6899 (2001).

[8] H. Ollivier and W. H. Zurek, Physical Review Letters **88**, 017901 (2001).

[9] A. Ferraro, L. Aolita, D. Cavalcanti, F. M. Cucchietti, and A. Acin, Phys. Rev. A **81**, 052318 (2010).

[10] B. Eastin, arXiv preprint arXiv:1006.4402 (2010).

[11] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **89**, 180402 (2002).

[12] A. Brodutch and D. R. Terno, Phys. Rev. A **81**, 062103 (2010).

[13] M. Piani, P. Horodecki, and R. Horodecki, Phys. Rev. Lett **100**, 090502 (2008).

[14] S. Luo and W. Sun, Phys. Rev. A **82**, 012338 (2010).

[15] S. Boixo, L. Aolita, D. Cavalcanti, K. Modi, and A. Winter, arXiv:quant-ph/1105.2768 (2011).

[16] D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani, and A. Winter, Phys. Rev. A **83**, 032324 (2011).

[17] V. Madhok and A. Datta, Phys. Rev. A **83**, 032323 (2011).

[18] A. Streltsov, H. Kampermann, and D. Bruß, Phys. Rev. Lett. **106**, 160401 (2011).

[19] M. Piani, S. Gharibian, G. Adesso, J. Calsamiglia, P. Horodecki, and A. Winter, Phys. Rev. Lett. **106**, 220403 (2011).

[20] T. K. Chuan, J. Maillard, K. Modi, T. Paterek, M. Paternostro, and M. Piani, Phys. Rev. Lett **109**, 070501 (2012).

[21] B. Dakic, Y. O. Lipp, X. Ma, M. Ringbauer, S. Kropatschek, S. Barz, T. Paterek, V. Vedral, A. Zeilinger, C. Brukner, and P. Walther, Nat. Phys. **8**, 666 (2012).

[22] M. Gu, H. Chrzanowski, S. Assad, T. Symul, K. Modi, T. Ralph, V. Vedral, and P. Lam, Nat. Phys. (2012).

[23] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, Phys. Rev. A **65**, 062324 (2002).

[24] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White, Phys. Rev. Lett. **95**, 210504 (2005).